Лабораторна робота № 4.

Виконали: студенти групи ФІ32мн Ємець Єлизавета
Карловський Володимир
Коваленко Дар'я

Тема: "Дослідження систем захисту захищених месенжерів типу Skype, Viber, WhatsApp, Signal".

Мета роботи: "Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP".

Завдання на лабораторну роботу

Група 1. Проаналізувати існуючу інформацію про системи Viber, WhatsApp, Skype, Telegram та їх криптографічні механізми. Детально розібрати опис усіх механізмів протоколу, структуру пакетів та характеристики систем. Довести теоретично можливість існування в системі виявлених протоколів та зробити огляд відомих аналізів захищеності вказаних протоколів, включаючи вже виправлені помилки. Зробити порівняльний аналіз можливостей вказаних систем, їх криптографічних механізмів та рівня захищеності (обґрунтований). Дати рекомендації користувачам щодо безпечного використання таких систем. Всю зібрану інформацію оформити у вигляді детального звіту з власним аналізом рівня захищеності та обраних криптографічних механізмів.

1. Загальний огляд систем Viber, WhatsApp, Skype і Telegram, їхнє призначення та функціональність

Viber, WhatsApp, Skype та Telegram є популярними месенджерами, призначеними для забезпечення миттєвої передачі текстових повідомлень, голосових та відеодзвінків, обміну медіафайлами та групових чатів. Їхня функціональність включає:

1. Текстові повідомлення: основний спосіб спілкування користувачів, який підтримують усі чотири системи.
2. Голосові та відеодзвінки: забезпечують аудіо- та відеозв'язок між користувачами в реальному часі.
3. Медіафайли: можливість обміну зображеннями, відео та документами.
4. Групові чати та дзвінки: підтримка обміну інформацією в групах, дозволяє одночасну взаємодію багатьох користувачів.

5. Додаткові функції безпеки: налаштування конфіденційності, двофакторна автентифікація, можливість видалення повідомлень, встановлення паролів на чати та інше.
- Роль криптографії в забезпеченні безпеки даних у цих системах

Криптографія є основним компонентом забезпечення безпеки даних у цих месенджерах, оскільки допомагає гарантувати:

- ❖ Конфіденційність
- ❖ Цілісність
- ❖ Автентифікація
- ❖ Контроль доступу

У месенджерах для захисту даних використовується наскрізне шифрування (end-to-end encryption), яке гарантує, що повідомлення шифруються на пристрої відправника і розшифровуються тільки на пристрої отримувача, залишаючись недоступними для третіх сторін (включаючи сервери месенджерів). Однак не всі системи реалізують повне наскрізне шифрування для всіх видів зв'язку, що робить їх рівень захисту неоднаковим.

2. Короткий огляд протоколів та характеристик систем

Viber

Протокол криптографії та end-to-end шифрування

- Viber застосовує end-to-end шифрування(E2E) для текстових повідомлень, голосових і відеодзвінків, а також передавання файлів.
- Для забезпечення захищеності даних у Viber використовується комбінація симетричного шифрування (AES-256) та асиметричного шифрування (RSA-2048). AES використовується для безпосереднього шифрування даних, а RSA для обміну ключами між користувачами.
- Ключі шифрування генеруються унікально для кожного сеансу зв'язку і зберігаються тільки на пристроях відправника та отримувача, що забезпечує конфіденційність.

Основні параметри захищеності

- Ідентифікація користувачів

Viber використовує цифрові відбитки (фінгерпринти) для підтвердження автентичності користувачів і перевірки ключів шифрування.

- Контроль безпеки ключів

Користувачі можуть вручну перевірити відбитки один одного, щоб переконатися у відсутності атак типу "людина посередині".

- Недоліки

Viber не відкриває свій протокол шифрування для зовнішнього аудиту, що обмежує можливість незалежного аналізу захищеності системи.

WhatsApp

WhatsApp використовує протокол Signal для наскрізного шифрування, який став стандартом завдяки своїй надійності та відкритості для перевірки. Signal забезпечує безпечний обмін даними шляхом встановлення сесійного ключа через асиметричне шифрування і динамічне оновлення ключів для кожного сеансу.

- Асиметричне шифрування (RSA, ECDSA)

WhatsApp застосовує RSA-2048 для асиметричного шифрування, яке використовується для передачі сесійних ключів, а також ECDSA (Elliptic Curve Digital Signature Algorithm) для цифрових підписів. Це підвищує рівень захищеності завдяки ефективності та надійності підпису на основі еліптичних кривих.

- Симетричне шифрування (AES) та хешування (HMAC-SHA256)

Для шифрування повідомлень використовується AES-256, що забезпечує високий рівень конфіденційності. Для верифікації цілісності даних

застосовується HMAC-SHA256, який генерує хеш-підпис повідомлення, що дозволяє отримувачу перевірити, що повідомлення не було змінено.

- Основні параметри захищеності

Кожна сесія має унікальний ключ шифрування, а зміна сесійних ключів у Signal забезпечує ефективний захист від перехоплення навіть у випадку компрометації попереднього ключа.

- Доступність незалежного аудиту

Протокол Signal є відкритим для аналізу безпеки та має високу репутацію серед експертів.

Skype

- Шифрування на основі TLS для захисту трафіку

Skype застосовує TLS (Transport Layer Security) для захисту даних під час передачі між клієнтами та серверами Microsoft. TLS гарантує конфіденційність передачі, але не забезпечує повного наскрізного шифрування, тому Microsoft має можливість отримати доступ до контенту повідомлень.

- Недоліки у відсутності повноцінного end-to-end шифрування

Відсутність E2E означає, що дані можуть бути доступні Microsoft, що є ризиком з точки зору конфіденційності. Через централізоване зберігання даних у Skype можливий доступ до інформації за запитом урядових органів або внаслідок зломів сервера. Skype підходить для загальних комунікацій, але не є оптимальним для конфіденційних розмов.

Telegram

- Протокол MTProto

Telegram використовує власний криптографічний протокол MTProto для шифрування даних. MTProto поєднує симетричне шифрування (AES-256)

для основного захисту повідомлень та асиметричне шифрування (RSA-2048) для обміну ключами, використовуючи алгоритм Diffie-Hellman для створення спільного секретного ключа.

Секретні чати Telegram реалізують end-to-end шифрування, але звичайні чати, що зберігаються на сервері, захищені тільки TLS і MTProto, що забезпечує конфіденційність від зовнішніх атак, але не від доступу Telegram до даних.

Секретні чати забезпечують наскрізне шифрування і доступні тільки на пристрої, де були ініційовані, тобто вони не зберігаються на серверах Telegram.

Telegram пропонує додаткові функції безпеки, як-от таймер для самознищення повідомлень, що підвищує конфіденційність.

- Робота з ключами та вразливості MTProto

MTProto 1.0 спочатку мав вразливості, які могли дозволити потенційні атаки на обмін ключами та маніпуляцію з даними, що привело до оновлення до версії MTProto 2.0 з підвищеною безпекою.

MTProto 2.0 усунув попередні вразливості, але його закритий характер обмежує можливість незалежного аудиту.

- Основні параметри захищеності

Секретні чати забезпечують високий рівень конфіденційності завдяки end-to-end шифруванню, але звичайні чати зберігаються на серверах Telegram.

Відсутність повного відкритого аудиту MTProto 2.0 може викликати сумніви щодо його безпеки, хоча наразі не було виявлено критичних уразливостей.

3. Опис та аналіз криптографічних механізмів

Viber

- Механізми шифрування

Симетричне шифрування (AES)	Асиметричне шифрування (RSA)
AES-256	○ RSA-2048

- Взаємодія між клієнтами та сервером

Наскрізне шифрування (E2E). Viber застосовує наскрізне шифрування для всіх текстових повідомлень, дзвінків і медіафайлів, які передаються між користувачами.

Обмін ключами. Кожен сеанс зв’язку між користувачами починається з обміну ключами за допомогою RSA-2048. Після успішного встановлення сесії обмін повідомленнями відбувається з використанням симетричного шифрування AES-256, що забезпечує високу швидкість шифрування та розшифрування.

Фінгерпринти. Viber надає користувачам можливість перевірити автентичність сеансу зв'язку, зіставляючи цифрові відбитки (фінгерпринти) ключів, що допомагає уникнути атак типу "людина посередині" (MITM).

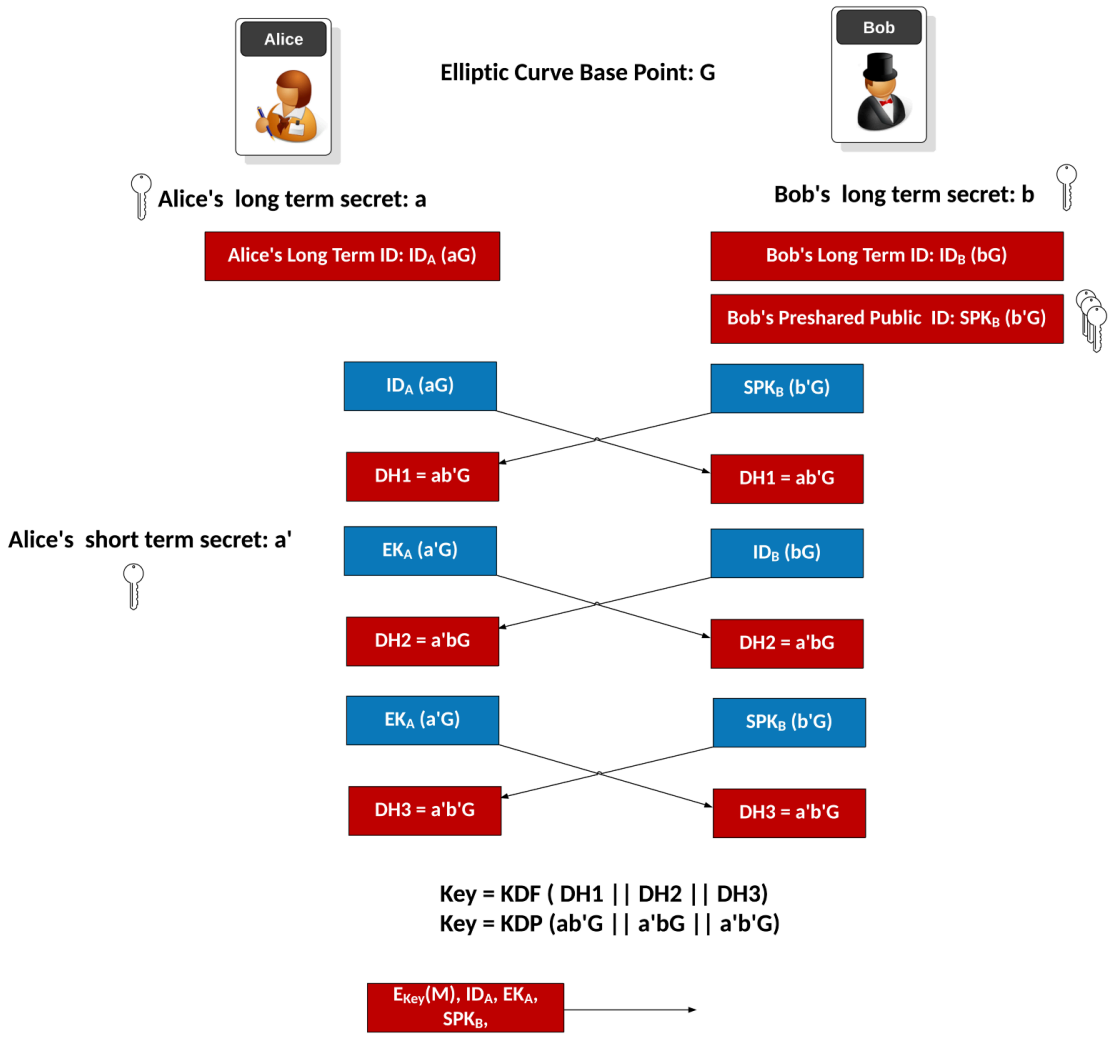
- Можливі уразливості
    - Атаки на пристрої користувачів
    - Атака MITM (людина посередині)
    - Відсутність незалежного аудиту
    - Слабкі місця в обміні ключами

Viber реалізує надійне наскрізне шифрування на основі AES-256 і RSA-2048, що забезпечує високий рівень конфіденційності для користувачів. Основні ризики пов'язані з безпекою кінцевих пристроїв і відсутністю прозорості щодо протоколу. Для покращення захисту Viber міг би надати протокол для зовнішнього аудиту та популяризувати серед користувачів перевірку фінгерпринтів для уникнення MITM-атак.

WhatsApp

WhatsApp використовує протокол Signal для забезпечення наскрізного шифрування (end-to-end encryption, E2E) повідомлень, дзвінків та медіафайлів, що є одним із найнадійніших відкритих криптографічних протоколів. Основні компоненти протоколу Signal у WhatsApp включають:

- Асиметричне шифрування для встановлення сесій
    - Алгоритм Діффі-Геллмана (Diffie-Hellman) використовується для створення початкового сеансового ключа. В рамках протоколу Signal використовується варіант цього алгоритму з еліптичними кривими, відомий як X3DH (Extended Triple Diffie-Hellman). X3DH дозволяє двом сторонам створити спільний секретний ключ, що використовується для шифрування даних, не обмінюючись ключами безпосередньо.



    - RSA-2048: асиметричне шифрування застосовується для передачі відкритих ключів і підписів, забезпечуючи автентифікацію під час встановлення з'єднання між користувачами.

Кожен користувач має постійний публічний та приватний ключі для ідентифікації, а також динамічні ключі, які змінюються з кожною новою сесією, що підвищує безпеку та запобігає компрометації навіть при тривалих комунікаціях.

- Каскадне оновлення ключів

Протокол Signal включає Double Ratchet Algorithm, який змінює сесійний ключ з кожним новим повідомленням. Це забезпечує, що навіть у разі компрометації одного з ключів, наступні повідомлення залишаються захищеними, оскільки використовуються інші ключі. Завдяки цьому алгоритму кожне повідомлення має унікальний ключ, що підвищує захищеність проти атак на цілісність сесії.

- Симетричне шифрування (AES)
    - WhatsApp використовує AES-256 для симетричного шифрування повідомлень у режимі CBC (Cipher Block Chaining), який забезпечує високу конфіденційність переданих даних. AES-256, з довжиною ключа 256 біт, вважається одним із найнадійніших алгоритмів шифрування.
    - Для забезпечення цілісності повідомлень використовується **HMAC-SHA256** (Hash-based Message Authentication Code). HMAC генерує хеш-підпис для кожного повідомлення, що дозволяє перевірити, чи не було воно змінено під час передачі.

- Відомі уразливості

1. Атака з використанням вразливості сервера

Протокол Signal передбачає наскрізне шифрування, але WhatsApp все одно має централізовані сервери для маршрутизації повідомлень і резервного

копіювання. Уразливості на стороні сервера можуть надати доступ до метаданих (наприклад, часу відправлення або отримувача повідомлення), навіть якщо сам вміст залишається зашифрованим.

2. Компрометація ключів сесії

Система кешування та зберігання ключів сесії може становити загрозу, якщо зловмисник отримає доступ до зашифрованих резервних копій, які зберігаються в Google Drive (для Android) або iCloud (для iOS). Ці резервні копії за замовчуванням не шифруються E2E, що дає можливість отримати доступ до повідомлень.

3. Метадані

Хоча повідомлення шифруються наскрізно, метадані про час відправлення, тривалість з'єднання та отримувача не захищені наскрізним шифруванням. Метадані можуть бути використані для аналізу зв’язків між користувачами та створення соціальних графів, що є загальною уразливістю для багатьох централізованих месенджерів.

Протокол Signal забезпечує високий рівень безпеки для WhatsApp завдяки використанню асиметричного шифрування для встановлення сесій та симетричного шифрування AES-256 для захисту повідомлень. Хоча протокол Signal дозволяє захистити вміст від сторонніх осіб, у WhatsApp все ще можуть виникати певні ризики, пов'язані з централізованим сервером та метаданими.

Для зниження ризиків WhatsApp додав підтримку E2E шифрування резервних копій і продовжує вдосконалювати захист даних, що робить його одним із найбільш захищених месенджерів для масового використання.

Skype

- TLS для шифрування трафіку між клієнтами та сервером

Transport Layer Security (TLS) використовується в Skype для шифрування даних під час передачі між клієнтами та серверами Microsoft. TLS гарантує захист переданого трафіку від перехоплення під час проходження через мережу.

Використання TLS забезпечує захист переданих даних від атак типу "людина посередині" (MITM) і перехоплення на маршруті між користувачем і сервером. TLS забезпечує безпеку передачі, але не гарантує захищеності даних на кінцевих пристроях.

- Відсутність повного end-to-end шифрування

На відміну від месенджерів із наскрізним шифруванням (end-to-end encryption, E2E), в яких дані шифруються на пристрої відправника та розшифровуються тільки на пристрої отримувача, Skype шифрує дані лише під час передачі між пристроєм користувача та сервером Microsoft.

Відсутність E2E шифрування означає, що контент повідомлень доступний серверу. Сервери Microsoft можуть обробляти, зберігати або переглядати дані в розшифрованому вигляді, що створює потенційний ризик витоку або доступу до приватного контенту.

Без E2E шифрування дані можуть бути збережені на сервері в зашифрованому вигляді (наприклад, резервні копії або тимчасове зберігання), але доступ до них все одно залишається у Microsoft. Це створює можливість для зловмисників або третіх сторін отримати доступ до даних за допомогою компрометації сервера або запитів з боку урядових органів.

- Проблеми з конфіденційністю

Через відсутність E2E шифрування Microsoft потенційно може отримати доступ до повідомлень та іншого контенту, що передається через Skype. Згідно з політикою конфіденційності Microsoft, компанія може переглядати

контент за необхідності для відповідності законодавству або для технічної підтримки.

Державні органи або інші уповноважені інстанції можуть подавати запити до Microsoft з вимогою надати доступ до даних користувачів. У таких випадках Microsoft, маючи доступ до контенту, може бути зобов’язана надати доступ до повідомлень відповідно до закону.

Через централізовану обробку даних і можливість доступу Microsoft Skype підходить для загальних комунікацій, але не для конфіденційних або чутливих даних, оскільки контент може бути збережений і доступний для внутрішніх перевірок.

Skype використовує TLS для захисту трафіку між клієнтами і сервером, що забезпечує базовий рівень захисту під час передачі. Проте відсутність наскрізного шифрування (E2E) означає, що Microsoft може отримувати доступ до повідомлень та інших даних, що створює ризики з точки зору конфіденційності. Skype забезпечує безпеку передачі, але не є ідеальним вибором для обміну конфіденційними даними через відсутність повного E2E шифрування і можливий доступ до контенту з боку Microsoft або за запитами третіх сторін.

Telegram

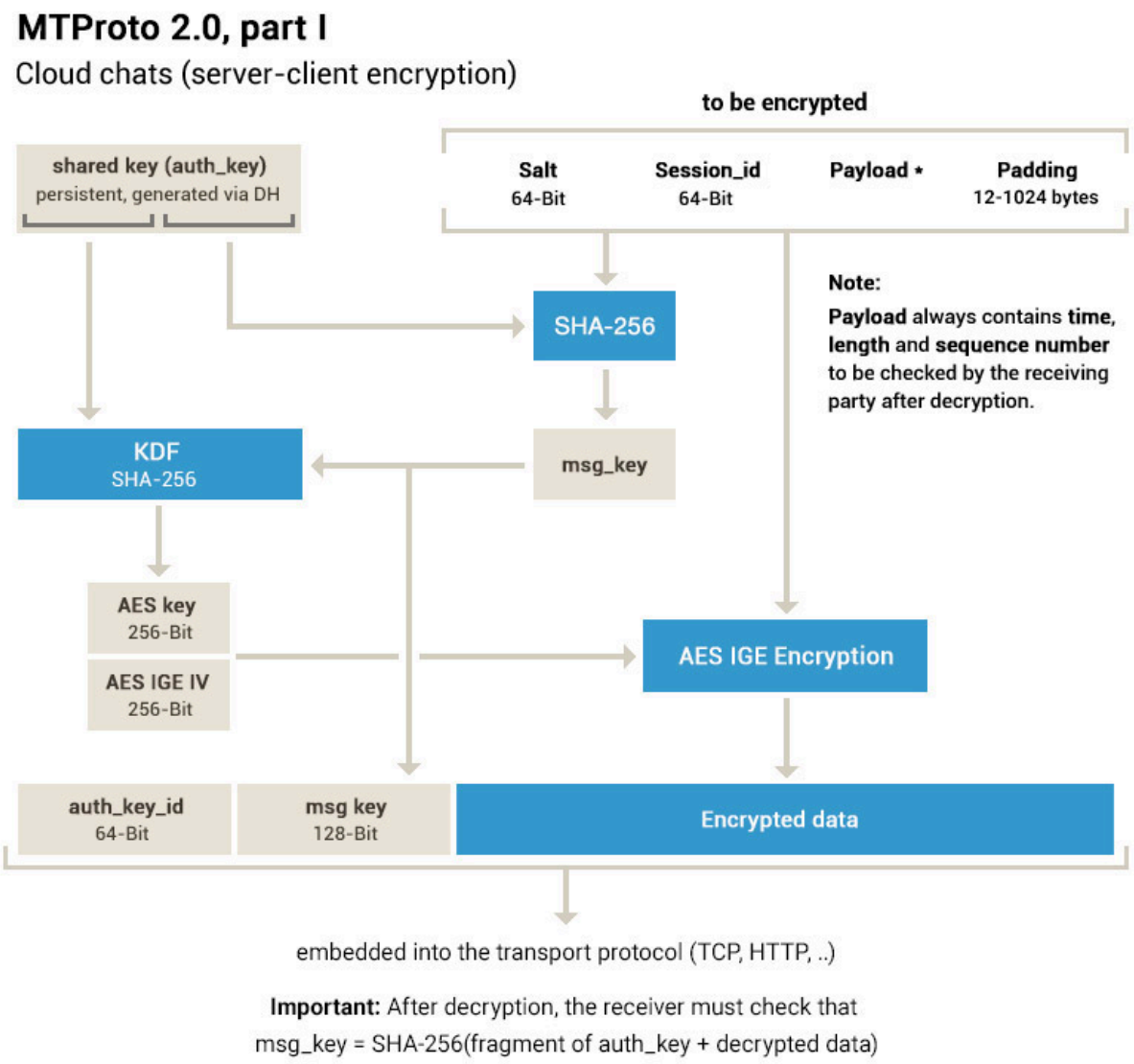
Telegram використовує власний протокол MTProto для забезпечення захищеності даних. MTProto поєднує кілька криптографічних механізмів для шифрування даних та автентифікації, включаючи:

- Симетричне шифрування (AES-256). Для захисту контенту повідомлень у MTProto використовується AES-256 у режимі IGE (Infinite Garble Extension). AES-256 забезпечує надійний рівень захищеності, зберігаючи дані конфіденційними під час передачі.
- MTProto використовує алгоритм Diffie-Hellman для створення спільного секретного ключа між клієнтами. Це дозволяє

користувачам створити спільний ключ для зашифрованої комунікації без передачі ключа напряму, що захищає їх від перехоплення.

- Асиметричне шифрування (RSA). Telegram використовує RSA-2048 для автентифікації і шифрування під час передачі ключів. RSA допомагає гарантувати, що обмін ключами між сервером і користувачами є захищеним.

Структура MTProto протоколу



MTProto складається з трьох основних компонентів: MTProto 1.0(первісна версія протоколу), MTProto 2.0(оновлена версія з виправленими

вразливостями) і MTProto Mobile Protocol (оптимізована версія для мобільних пристроїв).

Основна ідея MTProto — забезпечити безпечний обмін повідомленнями між користувачами та серверами Telegram, а також між користувачами, зберігаючи при цьому високу швидкість і зручність користування.

- Секретні чати з end-to-end шифруванням

Секретні чати в Telegram реалізують повне наскрізне шифрування (end-to-end encryption, E2E), що означає, що повідомлення шифруються на пристрої відправника і розшифровуються тільки на пристрої отримувача. Це забезпечує, що навіть сервери Telegram не можуть отримати доступ до контенту секретних чатів.

- Обмеження MTProto

Звичайні чати (несеансові) в Telegram не використовують E2E шифрування. Дані в таких чатах шифруються тільки на рівні передачі між клієнтом і сервером, що дає Telegram можливість зберігати повідомлення на своїх серверах і синхронізувати їх між пристроями користувача.

Обмеження E2E тільки в секретних чатах робить Telegram менш захищеним для звичайних чатів у порівнянні з месенджерами, які реалізують E2E шифрування за замовчуванням для всіх комунікацій (наприклад, WhatsApp).

Відомі вразливості

1. MTProto 1.0

Перша версія MTProto (1.0) мала низку вразливостей, які ставили під загрозу конфіденційність і цілісність даних. Одна з основних проблем полягала у недостатньо надійному захисті від атак на цілісність даних, що могло призвести до їх зміни або втручання в обмін повідомленнями.

Протокол не використовував повний спектр сучасних стандартів криптографії для захисту від атак типу "людина посередині" (MITM), що

могло дозволити зловмиснику змінити або перехопити дані, особливо під час обміну ключами.

2. MTProto 2.0

У відповідь на критику та аналіз уразливостей MTProto 1.0, Telegram випустив MTProto 2.0. У цій версії були виправлені попередні слабкі місця та додані додаткові заходи безпеки, включаючи покращений захист цілісності даних і обробку ключів.

У MTProto 2.0 введені додаткові механізми для захисту від атак MITM і розширена криптографічна перевірка під час обміну ключами, що знижує можливість підміни даних і підвищує надійність автентифікації.

3. Обмежений зовнішній аудит

Telegram не є повністю відкритим для зовнішнього аудиту, що викликало певні сумніви щодо безпеки MTProto. Хоча протокол був розроблений для забезпечення високої швидкості та захисту, його закритий характер ускладнює можливість повної незалежної перевірки захищеності.

Попри численні оновлення та вдосконалення MTProto, Telegram критикували за відсутність стандартного підходу до E2E шифрування для всіх чатів, що могло б додати додатковий рівень захищеності.

4. Структура пакетів у системах

- **Формат та структура пакетів**: як виглядають пакети даних у кожній системі, які дані шифруються і де знаходяться заголовки.
- **Особливості форматування пакетів**: аналіз захищеності даних на рівні передачі, які дані можуть бути вразливими.

Skype

Заголовок: 96 біт
Тіло: змінна
Трейлер: 16 біт (Cyclic Redundancy Check)

Заголовок
ID пакету (16 біт)
Тип пакету (8 біт)
Прапорці (8 біт)
Довжина Тіла (32 біт)
Timestamp (32 біт)

Типи пакетів
Аудіо (0x01)
Відео (0x02)
Текст (0x03)
Службові (0x04)
Файли (0x05)

Viber

Заголовок: 64 біт
Тіло: змінна (зашифровано)
CRC: 32 біт (Cyclic Redundancy Check)

Заголовок

Версія протоколу (8 біт)
Тип повідомлення (8 біт)

Довжина даних (16 біт)
Sequence number (32 біт)

Шифрування
AES-256-CBC для payload
SHA256 для CRC

WhatsApp

Заголовок: 120 біт
Тіло: змінна (зашифровано)
HMAC: 32 біт

Компоненти заголовку

Версія протоколу (8 біт)
Тип контенту (8 біт)
ID отримувача (64 біт)
Timestamp (32 біт)
Флаги шифрування (8 біт)

Протокол шифрування: Signal Protocol, Двостороннє шифрування

Signal

Заголовок: 104 біт
Тіло: змінна (зашифровано)
HMAC: 64 біт

Компоненти заголовку
Версія протоколу (8 біт)
ID пристрою відправника (32 біт)
ID сесії (32 біт)
Лічильник повідомлень (32 біт)

Особливості безпеки
Double Ratchet Algorithm
X3DH для встановлення ключів
Signal Protocol
Двостороннє шифрування

5. Теоретичний аналіз вразливостей протоколів та їх усунення

- **Виявлені уразливості та вразливості протоколів**:
    - Виявлені уразливості кожної з систем (як-от слабкі місця Signal протоколу, обхід шифрування в MTProto 1.0).
- **Виправлення та оновлення протоколів**: огляд змін і вдосконалень у системах, які підвищили їхню захищеність.
- **Теоретична можливість атак**: розглядаються потенційні атаки на кожен протокол (людина посередині, атакуючий пристрій), а також рівень захищеності проти таких атак.

Signal Protocol (+ WhatsApp)

Проблема верифікації ключів (CVE-2019-9971)

1. Можливість підміни публічних ключів під час початкової установки
2. Ризик MITM-атаки при першому підключенні
3. Складність перевірки автентичності співрозмовника

Вразливість повторного використання ключів

1. Можливість повторного використання одноразових ключів
2. Ризик компрометації попередніх повідомлень

Виправлення

Проблема верифікації ключів (CVE-2019-9971) була розв’язана за допомогою модифікації X3DH
Проблема повторного використання ключів та MITM частково вирішуються наступними методами:
1. Safety Numbers для перевірки ключів
2. QR-коди для очної верифікації
3. Автоматичне оновлення ключів кожні 14 днів

Telegram (MTProto)

MTProto 1.0
Криптографічні недоліки: Власна реалізація криптографії, Вразливість у схемі авторизації, Можливість атак на основі обраного шифротексту.

https://mtpsym.github.io/

Виправлення

У версії MTProto 2.0 було виправлено вразливість від активних атак (IND-CCA)

Окремо які є підходи до вирішення загальних вразливостей:
MITM (Man-in-the-Middle)

Вектор атаки: Перехоплення початкового обміну ключами
Захист: детекція
1. QR-код верифікація
2. Safety numbers

Replay-атаки

Вектор атаки: Повторне відправлення перехоплених повідомлень
Захист:
1. Timestamp перевірка
2. Унікальні ідентифікатори повідомлень
3. Лічильники послідовності

Компрометація пристрою

Вектор атаки: Фізичний доступ до пристрою
Захист:
1. Локальне шифрування бази даних
2. Захист від експорту ключів
3. Автоматичне видалення старих повідомлень

6. Порівняльний аналіз можливостей систем

- **Конфіденційність**: наскільки дані захищені від перехоплення, оцінка наскрізного шифрування (e2e).
- **Ідентифікація та аутентифікація користувачів**: надійність обміну ключами, захищеність проти атак на ідентифікацію.
- **Контроль доступу**: рівень безпеки доступу до даних, які типи атак можливі в разі компрометації пристроїв.
- **Додаткові заходи безпеки**: такі як двофакторна автентифікація, повідомлення про зміну ключів, можливість резервного копіювання в зашифрованому вигляді.

Конфіденційність

Мессенджер	Переваги	Недоліки
Signal	Наскрізне шифрування для всіх типів повідомлень	Мінімальний збір метаданих
	Регулярна ротація ключів	
WhatsApp	Наскрізне шифрування за замовчуванням	Збір метаданих для аналітики
	Регулярна ротація ключів	Резервні копії можуть бути вразли
Telegram	Наскрізне шифрування тільки в секретних чатах	Власний протокол шифрування
		Зберігання повідомлень на серверах

Ідентифікація та аутентифікація

Мессенджер	Нюанс ідентифікації та аутентифікації
Signal	Extended Triple Diffie-Hellman (X3DH)
	Криптографічні відбитки пристроїв
	Виявлення зміни ключів (Safety Numbers)

WhatsApp	Extended Triple Diffie-Hellman (X3DH)
	Верифікація через QR-код
Telegram	2FA з паролем
	Управління активними сесіями

Контроль доступу

Мессенджер	Функціонал контролю доступу
Signal	Локальне шифрування бази даних
	Неможливість експорту ключів
	Віддалене очищення історії
WhatsApp	Обмеження пересилання
	Контроль доступу до медіафайлів
Telegram	Детальне управління правами
	Локальний пароль
	Віддалене завершення сесій

7. Рекомендації користувачам щодо безпечного використання систем

Загальні поради

Уникнення відкритих Wi-Fi мереж:

- Категорична заборона використання відкритих Wi-Fi мереж для передачі конфіденційних даних
- Обов'язкове використання корпоративних VPN-рішень при роботі через публічні мережі
- Пріоритетне використання захищених мобільних мереж для критично важливих комунікацій
- Впровадження методів верифікації автентичності Wi-Fi мереж у публічних локаціях

Захист домашньої мережі:

- Імплементація комплексних парольних політик з мінімальною довжиною 14 символів
- Встановлення регулярних циклів ротації криптографічних ключів
- Обов'язкове використання WPA3-Enterprise для корпоративних мереж
- Регулярне оновлення мережевого обладнання та усунення вразливостей
- Деактивація потенційно небезпечних сервісів (WPS, віддалене адміністрування)

Налаштування 2FA:

- Обов'язкове впровадження на всіх критичних сервісах
- Регулярний аудит налаштувань та оновлення механізмів 2FA
- Використання апаратних ключів безпеки для критичних систем

Загальні налаштування безпеки:

- Впровадження систем централізованого управління оновленнями

- Використання корпоративних рішень для захисту від шкідливого ПЗ
- Конфігурація автоматичного блокування пристроїв згідно політик безпеки
- Обов'язкове шифрування локальних сховищ даних
- Впровадження автоматизованих систем резервного копіювання

Особливості безпеки окремих систем

- Для **Viber**: рекомендоване використання двофакторної автентифікації та обмеження доступу до пристрою.
- Для **WhatsApp**: рекомендації щодо регулярного підтвердження безпеки ключів, використання збереження даних у зашифрованому вигляді.
- Для **Skype**: обмеження використання для передавання конфіденційної інформації через відсутність повного e2e шифрування.
- Для **Telegram**: використання секретних чатів для передачі важливих даних і рекомендації щодо захисту облікового запису.

Порівняльна таблиця безпеки месенджерів

Функція безпеки	**Viber**	**WhatsApp**	**Skype**	**Telegram**
E2E шифрування	Так	Так	Частково	У секретних чатах
2FA	Так		Так	Так
Секретні чати	Ні	Ні	Ні	Так
Захист від скріншотів	Так	Ні	Ні	У секретних чатах
Шифровані резервні копії	Ні	Так	Ні	Так

8. Висновки

Аналіз рівня захищеності та обраних криптографічних механізмів

Рівні захищеності систем:

WhatsApp:

- Імплементація протоколу Signal забезпечує криптографічну стійкість через використання AES-256
- Механізм Perfect Forward Secrecy гарантує, що компрометація одного ключа не призведе до розкриття попередніх комунікацій
- Верифікація криптографічних ключів через QR-коди знижує ризик MITM-атак
- Відсутність контролю над метаданими створює потенційні ризики при комерційному використанні

Telegram:

- Пропрієтарний протокол MTProto 2.0 використовує гібридне шифрування (AES-256 + RSA-2048)
- Архітектура з наскрізним шифруванням виключно в секретних чатах створює потенційну вразливість
- Реалізовані механізми протидії MITM-атакам підвищують загальний рівень безпеки
- Централізоване зберігання даних на серверах становить потенційний ризик при компрометації інфраструктури

Viber:

- Власна імплементація E2EE з Perfect Forward Secrecy забезпечує достатній рівень захисту
- Комплексне шифрування всіх типів контенту підвищує загальну безпеку системи
- Механізми верифікації контактів знижують ризики соціальної інженерії

- Обмежена прозорість технічної реалізації ускладнює незалежний аудит безпеки

Skype:

- Базовий захист на рівні TLS без повноцінного E2EE створює суттєві ризики
- Інтеграція з екосистемою Microsoft накладає додаткові обмеження на конфіденційність
- Відсутність сучасних криптографічних механізмів робить систему вразливою
- Централізована архітектура підвищує ризики масової компрометації даних

Переваги та недоліки кожної системи

WhatsApp

Переваги	**Недоліки**
Надійне наскрізне шифрування всіх повідомлень	Прив'язка до номера телефону
Відкритий протокол Signal з доведеною безпекою	Обмежені можливості керування приватністю
Автоматична верифікація ключів	Належність до Meta викликає питання щодо збору метаданих
Широка підтримка різних типів повідомлень	Обмежені можливості використання на кількох пристроях

Telegram

Переваги	**Недоліки**

Гнучкі налаштування приватності	Наскрізне шифрування тільки в секретних чатах
Потужні можливості групових комунікацій	Закритий протокол шифрування
Відмінна підтримка мультимедіа	Зберігання повідомлень на серверах
Можливість використання без номера телефону	Питання щодо безпеки власного протоколу

Viber

Переваги	**Недоліки**
Вбудоване наскрізне шифрування	Менш прозора система безпеки
Додаткові функції безпеки	Обмежені можливості верифікації
Зручний інтерфейс	Залежність від номера телефону
Широкі можливості групових комунікацій	Менша увага до приватності метаданих

Skype

Переваги	**Недоліки**
Інтеграція з екосистемою Microsoft	Відсутність повного наскрізного шифрування
Надійна система автентифікації	Обмежені можливості захисту приватності
Широкі можливості для відеозв'язку	Централізована архітектура
Професійні функції для бізнесу	Можливість доступу до даних з боку Microsoft

Перспективи вдосконалення

1. Квантова криптографія та пост-квантові алгоритми:
    - Впровадження квантово-стійких алгоритмів шифрування
    - Розробка гібридних криптосистем для захисту від квантових атак
    - Дослідження та імплементація квантового розподілу ключів
2. Захист метаданих та анонімізація:
    - Впровадження технологій zero-knowledge proof
    - Розвиток протоколів анонімної маршрутизації
    - Мінімізація цифрового сліду користувачів
3. Вдосконалення користувацького контролю:
    - Імплементація гранулярного контролю над даними
    - Розробка механізмів верифікованого видалення інформації
    - Впровадження прозорих систем аудиту безпеки
4. Стандартизація та регуляторна відповідність:
    - Уніфікація протоколів безпеки
    - Забезпечення відповідності GDPR та іншим регуляторним вимогам
    - Розробка галузевих стандартів безпеки
5. Організаційна безпека:
    - Впровадження систем управління інформаційною безпекою (СУІБ)
    - Регулярний аудит безпеки та тестування на проникнення
    - Розробка політик реагування на інциденти

В цілому, розвиток систем обміну повідомленнями повинен відбуватися у напрямку посилення захисту приватності користувачів при збереженні зручності використання. Це вимагає постійного вдосконалення технологій шифрування, розвитку механізмів захисту від нових загроз та підвищення прозорості систем безпеки.